From:	ehud barak <ehbarak1@gmail.com>
To:	Gary Fegel <gary@fegel.com>
CC:	
Date:	Fri, 9/27/2013 1:13:02 AM
Subject:	Fwd: Lockheed to Boeing Building Security-Industrial Complex

Hi Gary
an old piece I've bumped into in my archive. worth reading. did you talk to Pavel? Hag Sameach.
EB

Begin forwarded message:

> **From:** ehud barak <ehbarak1@gmail.com>
> **Subject: Lockheed to Boeing Building Security-Industrial Complex**
> **Date:** June 11, 2013 8:11:09 AM GMT+03:00
> **To:** barak ehud <Ehbarak1@gmail.com>
>
> Lockheed to Boeing Building Security-Industrial Complex
>
> The front line in America's battle to fight computer hackers from China and master electronic warfare isn't on a far-away battlefield or at a diplomatic retreat.
>
> It's in the rolling suburbs of Maryland outside Washington.
>
> While President Barack Obama discussed cybersecurity with Chinese President Xi Jinping in California last week, defense contractors led by Lockheed Martin Corp. (LMT) and computer security companies were working alongside the U.S. Cyber Command and the National Security Agency (0053520D) to thwart digital attacks while the military pursues offensive capabilities.
>
> A half-century after President Dwight D. Eisenhower warned of the dangers of the "military-industrial complex" -- the monetary ties between lawmakers, armed forces and contractors -- some privacy and civil liberties advocates see a digital equivalent developing 25 miles from the White House.
>
> "The cybersecurity-industrial complex is focused on making money," said Sascha Meinrath, vice president of the New America Foundation, a Washington-based policy group. "It is directly making us far less safe as it careens blindly into territory that all but guarantees reprisals and collateral damage."
>
> Congress and the White House haven't set terms for online threat sharing between government and the private sector or the development of weapons like the Stuxnet computer worm that hit Iran's nuclear facilities, Meinrath said.
>
> Officials of companies that had moved there see the proximity between campuses of defense contractors, technology security companies and government defense and intelligence agencies -- some so close workers can walk between them -- as a way to better protect the U.S. Maryland Governor Martin O'Malley, a Democrat, calls it the "Silicon Valley of cybersecurity."
>
> **Cybersecurity Complex**

At Lockheed's 25,000-square-foot NexGen Cyber Innovation and Technology Center in Gaithersburg, Maryland, analysts work in rooms with entry controlled by biometric iris scans. Here, they use a technique known as the "cyber kill chain" to identify malicious computer code, part of an effort to defend against an estimated 2 billion monthly hacks on U.S. government networks.

The Pentagon in May accused the Chinese of intruding into U.S. computers to steal sensitive data and Obama in February approved an executive order allowing some information sharing on security threats between government and companies.

"Cybersecurity is a team sport," said retired Air Force General Charles Croom, cybersecurity solutions vice president at Bethesda, Maryland-based Lockheed and former director of the Defense Information Systems Agency, the U.S. military's global computer support. "We have the capabilities that we can offer the government to help them meet their mission needs."

Federal Presence

Congress's inability to agree on rules for what companies and agencies can do to combat hackers hasn't stopped the fight. "I think when Henry Ford built his car there probably weren't a lot of rules about traffic signals and speed limits," Croom said.

Ten centers dedicated to protecting government and private networks from attacks have opened in Maryland since 2009, including those operated by Boeing Co. (BA), based in Chicago; Science Applications International Inc.. (SAI) of McLean, Virginia; and General Dynamics Corp. (GD) and Northrop Grumman Corp. (NOC), both based in Falls Church, Virginia.

Maryland's congressional delegation led by Democratic Senator Barbara Mikulski, leader of the Senate Appropriations Committee, has helped secure federal money to support the expansion, such as $10 million in 2012 and again this year for the National Cybersecurity Center of Excellence in Rockville, Maryland. The center uses commercial technology to solve security challenges.

Fort Meade

Fort Meade, a 5,000-acre military installation located between Baltimore and Washington, has expanded since 2010 to include the Cyber Command, DISA and U.S. Fleet Cyber Command, the Navy's headquarters for computer security.

The Pentagon is creating teams to carry out offensive and defensive digital operations, Army General Keith Alexander, who heads both NSA and Cyber Command, told lawmakers in March.

On May 6, the NSA broke ground on a 600,000-square-foot computing center that will protect national security networks and provide intelligence and warnings about online threats, Vaneé Vines, an agency spokeswoman, said in an e-mail.

The growth of this public-private sector expands the capabilities of the NSA which, Obama confirmed last week, is collecting the telephone records of almost all Americans and e-mails and other digital content sent through nine Internet companies.

The NSA, which has about 42,000 government and contract workers, has been able to expand under the veil of "excessive secrecy" and without adequate congressional

oversight, Jameel Jaffer, deputy legal director of the American Civil Liberties Union, said in an interview.

“The government gets to decide what the law means and there’s no check on the government’s decision, and that gives the NSA an incredible amount of power,” Jaffer said.

Business Interests

Being near intelligence and defense agencies in Maryland creates business opportunities, Bryan Palma, Boeing’s vice president of cyber and security solutions, said in an interview. Boeing opened a 32,000-square-foot computer security center next to Fort Meade in 2011.

“It’s a very competitive market and you want to be there,” Palma said.

Lockheed Martin won a contract in 2012 valued as much as $4.6 billion to manage the Defense Department’s global data network, under which the company secures the communications of millions of users, including warfighters in the field and military installations globally.

“It’s the largest DoD network operation,” Lee Holcomb, Lockheed’s director of transformational technologies, said in an interview. “It is our largest cyber defense activity because we’re talking millions of users on that network.”

Operation Snort

SourceFire (FIRE), a security firm based in Columbia, Maryland, sells network intrusion detection and prevention products to the government and companies. Founder Martin Roesch said in an interview he started the company from his home in 2001, went public in 2007 and had $223.1 million in 2012 revenues.

The company’s signature product, Snort, protects Defense Department networks and automatically analyzes data for malware, Roesch said.

General Dynamics in March became the latest contractor to open a security center in Maryland. “The adversaries that we’re seeing in the commercial space are in many cases the same folks we’re seeing in the government space,” John Jolly, a vice president at the company, said in an interview.

Maryland had the fourth most technology workers in the nation in 2012, according to an annual report from TechAmerica, a Washington-based technology lobby.

Lockheed, Northrop Grumman and SAIC are among Maryland’s largest employers and have contributed to Mikulski’s campaign and political action committee from 2007 to 2012. The donations include $79,900 from Northrop Grumman; $40,000 from Lockheed; and $37,000 from SAIC, according to the Center for Responsible Politics, a Washington-based lobbying research group.

To contact the reporter on this story: Chris Strohm in Washington at cstrohm1@bloomberg.net

To contact the editor responsible for this story: Bernard Kohn at bkohn2@bloomberg.net
Find out more about Bloomberg for iPhone: http://m.bloomberg.com/iphone/

Sent from my iPhone